UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/600,547	06/20/2003	Masayuki Numao	JP920020102US1	6077

48813 7590 09/02/2009

LAW OFFICE OF IDO TUCHMAN (YOR)
ECM #72212
PO Box 4668
New York, NY 10163-4668

EXAMINER	
TOLENTINO, RODERICK	

ART UNIT	PAPER NUMBER
2439	

NOTIFICATION DATE	DELIVERY MODE
09/02/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

pair@tuchmanlaw.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/600,547
Filing Date: June 20, 2003
Appellant(s): NUMAO ET AL.

Ido Tuchman (45,924)
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 5/29/2009 appealing from the Office action mailed 9/24/2008.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,215,877	Matsumoto, Tatsuro	04-2001
5,610,981	Mooney et al.	03-1997

5,933,605	Kawano et al.	08-1999
6,169,802	Lerner et al.	01-2001
2001/0004736	Hirano et al.	06-2001

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1, 3, 4, 6 – 10, 20 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matsumoto U.S. Patent No. (6,215,877) in view of Hirano et al. U.S. PG-Publication (2001/0004736).

As per claims 1, 20 and 21, Matsumoto teaches a key management server for managing secret keys and public keys corresponding to given attribute values and a provider terminal for generating an encrypted content that can be decrypted by said user terminal having said attribute secret keys corresponding to given attributes by means of said public keys (Matsumoto, Col. 2 Lines 60 – 67 and Col. 3 Lines 1 – 5), wherein said provider terminal distributes said encrypted content and said user terminal decrypts said encrypted content decryptable by means of said attribute secret keys of its own (Matsumoto, Col. 4 Lines 57 – 67) but fails to teach a user terminal for accessing said key management server to obtain attribute secret keys generated based on said secret keys, said attribute secret keys corresponding to attributes identifying said user terminal. However, in an analogous art Hirano teaches a user terminal for accessing said key management server to obtain attribute secret keys generated based on said secret keys, said attribute secret keys corresponding to attributes identifying said user terminal (Hirano, Paragraph 0098, key based on user's information).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Hirano's method for facilitating legitimate use of digital content with Matsumoto's key management server and chat system because it offers the advantage of protecting computerized data from unauthorized access (Hirano, Paragraph 0006).

As per claim 3, Matsumoto teaches user terminal sends a set of attribute values indicating attributes of its own to said key management server; and said key management server generates said attribute secret keys unique to said user terminal based on, among said secret keys managed by said key management server, secret keys corresponding to the attribute values sent from said user terminal and sends said attribute secret keys to said user terminal (Matsumoto, Col. 4 Lines 37 – 49).

As per claim 4, Matsumoto as modified teaches a key storage for storing secret keys and public keys corresponding to predetermined attribute values; an attribute secret key generator for obtaining a set of given attribute values and generating attribute secret keys corresponding to said set of attribute values based on secret keys corresponding to said attribute values among said secret keys stored in said key storage (Matsumoto, Col. 2 Lines 60 – 67 and Col. 3 Lines 1 – 5), and a sending/receiving unit for receiving said set of attribute values from a given user terminal and sending said attribute secret keys generated by said attribute secret key generator to said user terminal (Matsumoto, Col. 4 Lines 57 – 67) wherein said attribute values identifying said user terminal (Hirano, Paragraph 0098, key based on user's information).

As per claim 6, Matsumoto teaches an encrypted content generator for encrypting said content based on said criteria keys (Matsumoto, Col. 9 Lines 45 – 65) and a sending unit for sending said encrypted content without specifying any recipient of said content via a network (Matsumoto, Col. 4 Lines 57 – 67) but fails to teach a criteria key generator for obtaining public keys corresponding to attribute values indicating attributes of a recipient to which a content is to be sent and using said public keys to generate criteria keys that can be decrypted by secret keys corresponding to said public keys. However, in an analogous art Hirano teaches a criteria key generator for obtaining public keys corresponding to attribute values indicating attributes of a recipient to which a content is to be sent and using said public keys to generate criteria keys that can be decrypted by secret keys corresponding to said public keys (Hirano, Paragraph 0098, key based on user's information).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Hirano's method for facilitating legitimate use of digital content with Matsumoto's key management server and chat system because it offers the advantage of protecting computerized data from unauthorized access (Hirano, Paragraph 0006).

As per claim 7, Matsumoto teaches criteria key generator combines, based on predetermined rules, criteria keys corresponding to the individual attribute values encrypted by using public keys corresponding to said individual attribute values to generate a criteria key for restricting recipients of said content (Matsumoto, Col. 4 Lines 37 – 49).

As per claim 8, Matsumoto disclose criteria key generator generates a session key for encrypting said content and a criteria key for decrypting said session key; and said encrypted content generator uses said session key to encrypt said content content (Matsumoto, Col. 4 Lines 37 – 49).

As per claim 9, Matsumoto teaches a sending/receiving unit for accessing a key management server managing (Matsumoto, Col. 4 Lines 57 – 67) and a decryptor for obtaining an encrypted content and decrypting said content based on said attribute secret keys (Matsumoto, Col. 11 Lines 2 – 8) but fails to teach secret keys and public keys corresponding to given attribute values to receive attribute secret keys corresponding to attributes established for identifying said information processing apparatus, said attribute secret keys being generated based on said secret keys. However, in an analogous art Hirano teaches teach secret keys and public keys corresponding to given attribute values to receive attribute secret keys corresponding to attributes established for identifying said information processing apparatus, said attribute secret keys being generated based on said secret keys (Hirano, Paragraph 0098, key based on user's information).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Hirano's method for facilitating legitimate use of digital content with Matsumoto's key management server and chat system because it offers the advantage of protecting computerized data from unauthorized access (Hirano, Paragraph 0006).

As per claim 10, Matsmoto teaches sending/receiving unit sends a set of attribute values established for said information processing apparatus to said key management server and receives said attribute secrete keys generated based on said set of attribute values from said key management server (Matsumoto, Col. 4 Lines 37 – 49).

Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Matsumoto U.S. Patent No. (6,215,877) and Hirano et al. U.S. PG-Publication (2001/0004736), as applied to claim 1 and in further view of Kawano et al. U.S. Patent No. (5,933,605).

As per claim 2, Matsumoto fails to teach provider terminal distributes said encrypted content without specifying said user terminal that is to receive said encrypted content. However, in an analogous art Kawano teaches provider terminal distributes said encrypted content without specifying said user terminal that is to receive said encrypted content (Kawano, Col.11 Lines 40 – 57).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Kawano's apparatus for filtering multicast messages with Matsumoto's key management server and chat system because it offers the advantage of have the data receiving operation that is not dependent on an expansion system (Kawano, Col.11 Lines 40 – 57).

Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Matsumoto U.S. Patent No. (6,215,877) and Hirano et al. U.S. PG-Publication (2001/0004736), and in view of Applicant Admittance Prior Art (hereafter AAPA).

As per claim 5, Matsumoto in view of Hirano fails to teach attribute secret key generator generates said attribute secret keys by using a protocol implementing oblivious transfer protocol. However, attribute secret key generator generates said attribute secret keys by using a protocol implementing oblivious transfer is taught by applicant on pages 14 and 15. The specification describes oblivious transfer protocol, in order to be used secretly obtain attribute secret keys.

(10) Response to Argument

Response to Section I)

Appellant argues on pages 6 and 7, that "the term attribute as used herein refers to information representing the individuality of the user of a user terminal or the user terminal itself," should entail that the term attribute must be interpreted by what is in the specification. This limitation is not in the claim. The limitations of claim 1, were given the broadest reasonable interpretation consistent with the specification, as noted in MPEP 2111. The interpretation of the Examiner of keys based on user ID or passwords as cited by Hirano on Paragraph 0098, is consistent with a reasonable interpretation of the limitation.

Appellant argues on pages 7 and 8, that Matsumoto in view of Hirano fails to disclose, teach or even suggest "a user terminal for accessing said key management

server to obtain attribute secret keys generated based on said secret keys, said attribute secret keys corresponding to attributes identifying said user terminal," regarding claim 1. Examiner respectfully disagrees. Matsumoto fails to teach a user terminal for accessing said key management server to obtain attribute secret keys generated based on said secret keys, said attribute secret keys corresponding to attributes identifying said user terminal. However, in an analogous art Hirano teaches a user terminal for accessing said key management server to obtain attribute secret keys generated based on said secret keys, said attribute secret keys corresponding to attributes identifying said user terminal (Hirano, Paragraph 0098, key based on user's information). Appellant's argument was directed towards the idea that Hirano was fails to access a key management server to obtain a key. However, it was not the position of the Examiner to have Hirano teach this limitation. The primary reference (Matsumoto) was used to teach a key management server which is accessed and distribute keys. Hirano was used to teach that it is well known in the art to have a key which corresponds to another key which is based on user attributes (Hirano, Paragraph 0098). Which reads on the limitation of claim 1, where a key is generated based on another key/set of keys wherein those keys were based on user information and/or attributes. It was never the position of the Examiner to teach the key management server.

Further on Pages 8 and 9, Applicant argues that it would be improper to combine the references of Matsumoto and Hirano. Examiner respectfully disagrees. At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Hirano's method for facilitating legitimate use of digital content with

Matsumoto's key management server and chat system because it offers the advantage of protecting computerized data from unauthorized access (Hirano, Paragraph 0006). Hirano and Matsumoto both deal with the transmission of data by using encrypted means, which is reasonable enough to show that the two references are in an analogous art. It would be obvious to combine the two references, since Hirano is teaching a more secure key than what is in Matsumoto. Thus a more secure key would increase the protection of computerized data from unauthorized access from unauthorized parties.

Response to Section II)

Appellant argues on pages 11 and 12, that Matsumoto in view of Kawano is in error since the examiner failed to provide an explanation or reasoning for the rejection. Citing 37 C.F.R. 1.104 c (2). Examiner respectfully disagrees. Appellant is claiming that reference was to complex to see the nature of the rejection. The limitation of claim 2 states "provider terminal distributes said encrypted content without specifying said user terminal that is to receive said encrypted content." Kawano states "In the communication system using the contents code, the transmitting computer attaches to the transmission data the contents code corresponding to the contents of transmission data and then transmits the resultant data without recognizing the address of the party." It is clear and NOT complex in how Kawano states that a communication system transmits data without specifying a user terminal since the data sent did not recognize the address of the party. This reads on the limitation of claim 2, where a provider

terminal, which in Kawano is the transmitting computer, distributes content without specifying terminal to receive the data, which in Kawano is the party receiving the data where the address is not recognized.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Roderick Tolentino

/R. T./

Examiner, Art Unit 2439

Conferees:

Edan Orgad

/Edan Orgad/

Supervisory Patent Examiner, Art Unit 2439

Christopher Brown

/Christopher J Brown/

Primary Examiner, Art Unit 2439